Designing Digital Defenses

LINDA D. KOZARYN

BRUSSELS, Belgium — Defense experts are gearing up to face a new danger threatening America and its allies — cyberattacks.

The advent of the computer-based Information Age has opened the door to unconventional attacks since almost every aspect of modern life has become increasingly dependent on computers. Telecommunications, government operations, banking and finance, transportation, air traffic control, water supply systems, medical, police, fire and rescue — all are vulnerable to attack.

By the year 2000, experts predict one million networks will be connected to the Internet. About 350 million computers will have E-mail access. Nearly 20 trillion bits of data are now transmitted monthly, and this figure is doubling annually.

All it might take to disrupt the nation's power grids and other critical infrastructure are a home computer, a telephone line, digital dexterity, and a double dose of moxie. Right now, computer hackers are poking and prodding, trying to gain unauthorized access to national and private systems.

Recently, for example, two computer-wise California teen-agers succeeded in breaching an unclassified Pentagon defense network. Security experts believe critical systems could well become the targets of more than inquisitive children.

Terrorists, criminals, disgruntled employees, and even rogue states could launch much more serious cyberattacks. Rather than confront the United States or its allies on the battlefield, future foes may attack nations' infrastructures. DoD alone has about 2.1 million computers, 10,000 local area networks, and more than 100 long-distance networks.

"There are no borders in cyberspace," Deputy Defense Secretary John Hamre declared at a NATO conference in Vienna in June. "It is absolutely imperative that we prepare now to protect these systems."

Last year, DoD conducted Eligible Receiver, an exercise to determine U.S. vulnerability to computer attacks, Hamre told about 250 NATO and Partnership for Peace members attending the 15th NATO Workshop.

"We selected a small group of employees — 35 individuals," Hamre explained. "We gave them funds to buy computers from local stores. They were only allowed to use off-the-shelf software or software they could download from the Internet. They were given three months to find out if they could disrupt the infrastructure of the United States."

The results were startling, Hamre said. "We didn't let them take down the power system of the United States, but they could have done it." Defense officials learned it only requires modest know-how to seriously disrupt vital services like power distribution and telecommunications, he said.

"A small handful of capable computer specialists — a capability well within the reach of even moderately developed countries — using off-the-shelf technology and equipment, can now wage war against the largest country in the world," he said.

Hence, the United States is taking steps to protect its infrastructure. A presidential mandate calls for a plan to implement information assurance measures. It includes creating lead agencies to coordinate with private companies, and setting up a new national infrastructure protection center. The plan designates a coordinator for infrastructure protection on the National Security Council. Government officials are also setting up a national warning and analysis center and increasing funding for information assurance fivefold, Hamre said.

"This is a pressing problem because you can't solve it by yourself," Hamre said. "The Defense Department cannot solve this problem because we don't own the systems that are likely to be attacked. We have to develop partnerships with the private sector to get them to fix this problem."

Cooperation among NATO allies and partners is also vitally important, he said. "With this increasingly 'Interneted' world, we cannot accept vulnerabilities in our allies," he said. "The weakest link in the chain becomes the broken chain for us all."

Editor's Note: This information is in the public domain at http://www.defenselink.mil/news/ on the Internet.